

# 6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of : Confirmation No. 8418

Masato YAMAMICHI et al. : Docket No. 2001\_1845A

Serial No. 10/020,308 : Group Art Unit 2131

Filed December 18, 2001 :

CRYPTOCOMMUNICATION SYSTEM,  
TRANSMISSION APPARATUS,  
AND RECEPTION APPARATUS

**THE COMMISSIONER IS AUTHORIZED  
TO CHARGE ANY DEFICIENCY IN THE  
FEES FOR THIS PAPER TO DEPOSIT  
ACCOUNT NO. 23-0975**

**CLAIM OF PRIORITY UNDER 35 USC 119**

Assistant Commissioner for Patents,  
Washington, DC 20231

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2000-384835, filed December 19, 2000, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Masato YAMAMICHI et al.

By Michael S. Huppert

Michael S. Huppert  
Registration No. 40,268  
Attorney for Applicants

MSH/kjf  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
April 30, 2002

CERTIFIED COPY

PRIORITY DOCUMENT

日 本 国 特 許 庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年12月19日

出 願 番 号

Application Number:

特願2000-384835

出 願 人

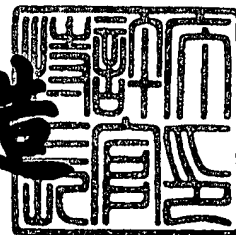
Applicant(s):

松下電器産業株式会社

2001年11月 2日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 2022520534

【提出日】 平成12年12月19日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 5/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 山道 将人

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 布田 裕一

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 大森 基司

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 館林 誠

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 データ暗号化システム、暗号装置、及び復号装置

【特許請求の範囲】

【請求項 1】 送信側と受信側で、予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、

送信側で、平文を、前記暗号鍵と前記一方向性関数に基づいて、暗号化して、暗号文を生成し、暗号文を受信側に送信し、

受信側では、前記暗号文を、前記復号鍵と一方向性関数に基づいて、復号し、復号文を入手するデータ暗号化システムであって、

前記送信側では、

前記平文を、前記暗号鍵に基づいて、暗号化部により暗号化し、第 1 の暗号部分情報を生成し、

前記平文を、前記一方向性関数に基づいて、第 1 の一方向性関数部により第 2 の暗号部分情報を生成し、

前記第 1 の暗号部分情報と前記第 2 の暗号部分情報を連結して、暗号文として前記受信側に送信する暗号装置を備え、

前記受信側では、

受信した前記暗号文のうち前記第 1 の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第 1 の復号部分情報を生成し、

前記第 1 の復号部分情報を、前記一方向性関数に基づいて、前記第 1 の一方向性関数部と同じ動作を行う第 2 の一方向性関数部により第 2 の復号部分情報を生成し、

前記第 2 の復号部分情報が前記第 2 の暗号部分情報と等しい場合は、前記第 1 の復号部分情報を復号文とする復号装置を備えることを特徴とするデータ暗号化システム。

【請求項 2】 平文を、前記暗号鍵に基づいて、暗号化部により暗号化し、第 1 の暗号部分情報を生成し、前記平文を、前記一方向性関数に基づいて、第 1 の一方向性関数部により第 2 の暗号部分情報を生成し、前記第 1 の暗号部分情報と前記第 2 の暗号部分情報を連結して、暗号文として送信することを特徴とする請求

項 1 に記載の暗号装置。

【請求項 3】受信した暗号文のうち第 1 の暗号部分情報を、請求項 1 に記載の復号鍵に基づいて、復号化部により復号し、第 1 の復号部分情報を生成し、前記第 1 の復号部分情報を、前記一方向性関数に基づいて、前記第 1 の一方向性関数部と同じ動作を行う第 2 の一方向性関数部により第 2 の復号部分情報を生成し、前記第 2 の復号部分情報が受信した暗号文のうちの第 2 の暗号部分情報と等しい場合は、前記第 1 の復号部分情報を復号文とすることを特徴とする請求項 1 に記載の復号装置。

【請求項 4】送信側と受信側で、予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、

送信側で、平文を、前記暗号鍵と一方向性関数に基づいて、暗号化して、暗号文を生成し、暗号文を受信側に送信し、

受信側では、前記暗号文を、前記復号鍵と前記一方向性関数に基づいて、復号し、復号文を入手するデータ暗号化システムであって、

前記送信側では、

前記平文に、情報付加部により付加情報を付加し、中間情報を生成し、

前記中間情報を、前記暗号鍵に基づいて、暗号化部により暗号化し、第 1 の暗号部分情報を生成し、

前記平文を、前記一方向性関数に基づいて、第 1 の一方向性関数部により第 2 の暗号部分情報を生成し、

前記第 1 の暗号部分情報と前記第 2 の暗号部分情報を連結して、暗号文として前記受信側に送信する暗号装置を備え、

前記受信側では、

受信した前記暗号文のうち前記第 1 の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第 1 の復号部分情報を生成し、

前記第 1 の復号部分情報から、情報除去部により前記付加情報を除去し、第 2 の復号部分情報を生成し、

前記第 2 の復号部分情報を、前記一方向性関数に基づいて、前記第 1 の一方向性関数部と同じ動作を行う第 2 の一方向性関数部により第 3 の復号部分情報を生

成し、

前記第 3 の復号部分情報が前記第 2 の暗号部分情報と等しい場合は、前記第 2 の復号部分情報を復号文とする復号装置を備えることを特徴とするデータ暗号化システム。

【請求項 5】平文に、情報付加部により付加情報を付加し、中間情報を生成し、前記中間情報を、前記暗号鍵に基づいて、暗号化部により暗号化し、第 1 の暗号部分情報を生成し、前記中間情報を、前記一方向性関数に基づいて、第 1 の一方向性関数部により第 2 の暗号部分情報を生成し、前記第 1 の暗号部分情報と前記第 2 の暗号部分情報を連結して、暗号文として送信することを特徴とする請求項 4 に記載の暗号装置。

【請求項 6】受信した暗号文のうち第 1 の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第 1 の復号部分情報を生成し、前記第 1 の復号部分情報から、情報除去部により前記付加情報を除去し、第 2 の復号部分情報を生成し、前記第 2 の復号部分情報を、前記一方向性関数に基づいて、前記一方向性関数部と同じ動作を行う第 2 の一方向性関数部により、第 3 の復号部分情報を生成し、前記第 3 の復号部分情報が受信した暗号文のうちの第 2 の暗号部分情報と等しい場合は、前記第 2 の復号部分情報を復号文とすることを特徴とする請求項 4 に記載の復号装置。

【請求項 7】前記暗号化部で用いられる暗号方式は、公開鍵暗号方式であることを特徴とする請求項 1 または請求項 4 に記載のデータ暗号化システム。

【請求項 8】前記第 1 の一方向性関数部で用いられる一方向性関数はハッシュ関数であることを特徴とする請求項 1 または請求項 4 に記載のデータ暗号化システム。

【請求項 9】前記第 1 の一方向性関数部で用いられる一方向性関数は、秘密鍵暗号方式の暗号化関数であることを特徴とする請求項 1 または請求項 4 に記載のデータ暗号化システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、復号時の誤り検出技術に関するものである。

#### 【0002】

##### 【従来の技術】

秘匿通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。暗号方式とは、この秘匿通信方式を実現するための一つの手段であり、簡単に説明すると、平文を暗号化するための暗号化アルゴリズムと暗号鍵、及び暗号文を復号するための復号アルゴリズムと復号鍵が存在して、暗号化アルゴリズムと暗号鍵を用いて平文を暗号化して送信し、復号アルゴリズムと復号鍵を用いて受信された暗号文を復号して復号文を得る方式である。暗号化アルゴリズムは、平文を入力として暗号文を出力するので、暗号化関数とも呼ばれる。また、復号アルゴリズムは、暗号文を入力として復号文を出力するので、復号化関数とも呼ばれる。暗号方式については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書に詳しく述べられている。

#### 【0003】

暗号方式の中に、正規の暗号鍵を用いて暗号化した暗号文を、正規の復号鍵を用いて復号しても、復号により得られた復号文が平文 $m$ と異なる可能性がある暗号方式がある。以降、正規の復号鍵を用いて復号しても、復号文が平文 $m$ と異なることを、「復号誤り」と記述し、復号誤りが生じる可能性がある暗号方式を、「復号誤りが発生し得る暗号方式」と記述する。

#### 【0004】

上記復号誤りが発生し得る暗号方式として、例えば、NTRU暗号方式がそれにあたる。この方式を簡単に説明すると、暗号鍵を用いて、平文を乱数をパラメータとして暗号化して暗号文を生成し、復号鍵を用いて、暗号文を復号して復号文を生成する方式である。この方式は、乱数をパラメータとして暗号化するので、平文が同じでも暗号文が異なる可能性があり、また、復号誤りが発生し得る方式である。NTRU暗号方式については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, “NTRU: A ring based public key cryptosystem”, Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998.



に詳しく述べられている。復号誤りが発生し得る暗号方式の一つである NTRU 暗号方式において、暗号鍵  $K_p$  を用いて暗号化する際に、乱数  $r$  をパラメータとして、平文  $m$  を暗号化した暗号文  $c$  を生成する関数を  $E$  で表し、入力  $m, K_p, r$  に対する出力が  $c$  であることを、

$$c = E(m, K_p, r)$$

で表す。また、復号鍵  $K_s$  を用いて、暗号文  $c$  から復号文  $m'$  を生成する関数を  $D$  で表し、入力  $c, K_s$  に対する出力が  $m'$  であることを、

$$m' = D(c, K_s)$$

で表す。

#### 【0005】

(従来例1)

以下に、上記復号誤りが発生し得る暗号方式を用いたデータ暗号化システム 3000 について、NTRU 暗号方式を例として、図 11～図 15 を用いて説明する。図 11 はデータ暗号化システム 3000 のブロック図であり、図 12 は暗号装置 3100 のブロック図であり、図 13 は暗号化部 3110 のブロック図であり、図 14 は復号装置 3200 のブロック図であり、図 15 は復号化部 3210 のブロック図である。暗号装置 3100 及び復号装置 3200 は、通信路 3300、例えば、無線通信路やインターネットなどで接続されているものとする。

#### 【0006】

また NTRU 暗号方式については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998. に詳しく述べられている。

#### 【0007】

(1) 鍵の生成

上記暗号方式を用いた通信を行う前に、適切な方法で上記暗号方式における復号鍵  $K_s$ 、及び暗号鍵  $K_p$  が生成されて、復号鍵  $K_s$  は復号化部 3210 に格納され、暗号鍵  $K_p$  は暗号化部 3110 に格納されているものとする。復号鍵  $K_s$ 、及び暗号鍵  $K_p$  の生成方法は、上記文献に述べられている。

## 【0008】

## (2) 暗号文の生成及び送信 (暗号装置 3100 の処理)

暗号化部 3110 は、NTRU 暗号方式の暗号化を行うものであり、乱数生成部 3112 で乱数  $r$  を生成し、予め格納されている暗号鍵  $K_p$  を用いて、平文  $m$  を暗号化関数部 3111 で、乱数  $r$  をパラメータとして暗号化し、暗号文  $c$  を生成する。即ち、

$$c = E(m, K_p, r)$$

そして、生成した暗号文  $c$  を送信部 3120 により、通信路 3300 へ送信する。

## 【0009】

## (3) 暗号文の受信及び復号 (復号装置 3200 の処理)

受信部 3220 は通信路 3300 から暗号文  $c$  を受信し、これを復号化部 3210 に送る。復号化部 3210 は、NTRU 暗号方式の復号を行うものであり、予め格納されている復号鍵  $K_s$  を用いて、受信した暗号文  $c$  を、復号化関数部 3211 で復号し、復号文  $m'$  を得る。即ち、

$$m' = D(c, K_s)$$

上記従来例 1 に示した復号誤りが発生し得る暗号方式を用いた暗号通信では、復号装置 3200 が暗号文を復号したときに、復号誤りのために暗号装置 3100 に入力された平文  $m$  を得られない場合がある。つまり、

$$m' = D(E(m, K_p, r), K_s)$$

とすると、復号誤りの発生のために、 $m' \neq m$  となる場合がある。

## 【0010】

復号誤りが発生しなかった場合、復号装置 3200 は受信した暗号文  $c$  から暗号装置 3100 に入力された平文  $m$  を出力することができるが、復号誤りが発生した場合、復号装置 3200 は、暗号装置 3100 に入力された平文  $m$  とは別のものを得ることになる。

## 【0011】

ここで、復号装置 3200 は、復号誤りの発生の有無に関わらず、暗号文  $c$  から何らかの復号文  $m'$  を出力することができるが、果たしてそれが暗号装置 31

00に入力された平文 $m$ と同一であるかどうかを判断することができない。つまり、受け取った暗号文を復号しても、その復号文は信頼がおけるかどうかを、復号装置を用いて判定できないことになる。

#### 【0012】

このように、この例では、復号装置は、受信した暗号文から得られた復号文 $m$ が、暗号装置3100に入力された平文 $m$ と同一であるかどうか判定できないため、データ暗号化システム3000においては意図した情報を確実に伝えることができないという問題がある。

#### 【0013】

##### (従来例2)

以下に、従来例1の上記問題を解決するための復号誤りが発生し得る暗号方式を用いたデータ暗号化システム4000について、NTRU暗号方式を例として、図16～図20を用いて説明する。図16はデータ暗号化システム4000のブロック図であり、図17は暗号装置4100のブロック図であり、図18は暗号化部4110のブロック図であり、図19は復号装置4200のブロック図であり、図20は復号化部4210のブロック図である。暗号装置4100、及び復号装置4200は、通信路4300で接続されている。

#### 【0014】

##### (1) 鍵の生成

上記暗号方式を用いた通信を行う前に、適切な方法で上記暗号方式における復号鍵 $K_s$ 、及び暗号鍵 $K_p$ が生成されて、復号鍵 $K_s$ は復号化部4210に格納され、暗号鍵 $K_p$ は暗号化部4110に格納されているものとする。復号鍵 $K_s$ 、及び暗号鍵 $K_p$ の生成方法は、上記文献に述べられている。

#### 【0015】

##### (2) 暗号文の生成及び送信(暗号装置4100の処理)

暗号化部4110は、NTRU暗号方式の暗号化を行うものであり、乱数生成部4112で乱数 $r$ を生成し、予め格納されている暗号鍵 $K_p$ を用いて、平文 $m$ を暗号化関数部4111で、乱数 $r$ をパラメータとして暗号化し、暗号文 $c = E(m, K_p, r)$ を生成するものである。

## 【0016】

暗号装置4100は、平文 $m$ を暗号化部4110により $n$ 回（ $n$ は2以上の整数）暗号化して、 $n$ 個の暗号文 $c[1]$ ， $c[2]$ ， $\dots$ ， $c[n]$ を生成する。即ち、

$$c[1] = E(m, K_p, r[1])$$

$$c[2] = E(m, K_p, r[2])$$

$\dots$

$$c[n] = E(m, K_p, r[n])$$

ここで $r[1]$ ， $r[2]$ ， $\dots$ ， $r[n]$ は、上記乱数生成部4112で生成される乱数とする。そして、生成した $n$ 個の暗号文 $c[1]$ ， $c[2]$ ， $\dots$ ， $c[n]$ を送信部4120により、通信路4300へ送信する。

## 【0017】

## (3) 暗号文の受信及び復号（復号装置4200の処理）

受信部4220は、暗号文 $c[1]$ ， $c[2]$ ， $\dots$ ， $c[n]$ を受信し、これらを復号化部4210に送る。復号化部4210は、NTRU暗号方式の復号を行うものであり、予め格納されている復号鍵 $K_s$ を用いて、受信した暗号文 $c[1]$ ， $c[2]$ ， $\dots$ ， $c[n]$ を、それぞれ復号化関数部4211で復号し、復号文 $m'[1]$ ， $m'[2]$ ， $\dots$ ， $m'[n]$ を得る。即ち、

$$m'[1] = D(c[1], K_s)$$

$$m'[2] = D(c[2], K_s)$$

$\dots$

$$m'[n] = D(c[n], K_s)$$

## (4) 復号誤りの検出

復号装置4200は比較部4230を用いて、上記のようにして得られた復号文 $m'[1]$ ， $m'[2]$ ， $\dots$ ， $m'[n]$ が一つでも異なっていたら復号誤りが発生したとみなし、 $j=0$ 、それ以外は $j=1$ とし、 $m'[1]$ ， $m'[2]$ ， $\dots$ ， $m'[n]$ ， $j$ を出力する。

## 【0018】

上記の従来例2は、従来例1に比べ、復号誤りを検出できるという利点がある

。しかし、この方法を用いると、通信量が従来例 1 の  $n$  倍になり、非効率的である。さらに、異なる乱数をパラメータとして同じ平文を暗号化した複数の暗号文を送信することにより、暗号方式の安全性が低下する恐れもある。これは、

$$c[1] = E(m, K_p, r[1])$$

$$c[2] = E(m, K_p, r[2])$$

...

$$c[n] = E(m, K_p, r[n])$$

の  $n$  個の関係式から平文  $m$  や乱数  $r[1]$ ,  $r[2]$ , ...,  $r[n]$  に関する情報が第三者に漏れる恐れがあるからである。このことを利用した暗号攻撃法を、Multiple Transmission Attack と言う。

#### 【0019】

具体的には、復号誤りの発生し得る暗号方式の 1 つである NTRU 暗号方式を用いて、上記復号誤り検出を行うと安全性が低下することが知られている。この攻撃法については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998. に詳しく述べられている。

#### 【0020】

##### 【発明が解決しようとする課題】

暗号システムにおいて、平文を相手に正しく伝えることが重要なのは言うまでもない。復号誤りの発生し得る暗号方式においては、復号誤りを検出することが最低限必要である。従来技術においては、復号誤りを検出しようとする、通信量が増大し、しかも安全性が低下する恐れもある。

#### 【0021】

本発明は、以上の従来技術における問題点を鑑みて行われたもので、データ暗号化システムにより、安全で効率的に復号誤りを検出する技術を提供することを目的とする。

#### 【0022】

##### 【課題を解決するための手段】

上記課題を解決するために、請求項1における発明は、送信側と受信側で、予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、送信側で、平文を、前記暗号鍵と一方向性関数に基づいて、暗号化して、暗号文を生成し、暗号文を受信側に送信し、受信側では、前記暗号文を、前記復号鍵と前記一方向性関数に基づいて、復号し、復号文を入手するデータ暗号化システムであって、前記送信側では、前記平文を、前記暗号鍵に基づいて、暗号化部により暗号化し、第1の暗号部分情報を生成し、前記平文を、前記一方向性関数に基づいて、第1の一方向性関数部により第2の暗号部分情報を生成し、前記第1の暗号部分情報と前記第2の暗号部分情報を連結して、暗号文として前記受信側に送信する暗号装置を備え、前記受信側では、受信した前記暗号文のうち前記第1の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第1の復号部分情報を生成し、前記第1の復号部分情報を、前記一方向性関数に基づいて、前記第1の一方向性関数部と同じ動作を行う第2の一方向性関数部により第2の復号部分情報を生成し、前記第2の復号部分情報が前記第2の暗号部分情報と等しい場合は、前記第1の復号部分情報を復号文とする復号装置を備えることを特徴とする。

## 【0023】

請求項2における発明は、請求項1に記載の暗号装置は、平文を、請求項1に記載の暗号鍵に基づいて、暗号化部により暗号化し、第1の暗号部分情報を生成し、前記平文を、請求項1に記載の一方向性関数に基づいて、第1の一方向性関数部により第2の暗号部分情報を生成し、前記第1の暗号部分情報と前記第2の暗号部分情報を連結して、暗号文として送信することを特徴とする。

## 【0024】

請求項3における発明は、請求項1に記載の復号装置は、受信した暗号文のうち第1の暗号部分情報を、請求項1に記載の復号鍵に基づいて、復号化部により復号し、第1の復号部分情報を生成し、前記第1の復号部分情報を、請求項1に記載の一方向性関数に基づいて、請求項1に記載の第1の一方向性関数部と同じ動作を行う第2の一方向性関数部により第2の復号部分情報を生成し、前記第2の復号部分情報が受信した暗号文のうちの第2の暗号部分情報と等しい場合は、前記第1の復号部分情報を復号文とすることを特徴とする。

## 【 0 0 2 5 】

請求項 4 における発明は、送信側と受信側で、予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、送信側で、平文を、前記暗号鍵と一方向性関数に基づいて、暗号化して、暗号文を生成し、暗号文を受信側に送信し、受信側では、前記暗号文を、前記復号鍵と前記一方向性関数に基づいて、復号し、復号文を入手するデータ暗号化システムであって、前記送信側では、前記平文に、情報付加部により付加情報を付加し、中間情報を生成し、前記中間情報を、前記暗号鍵に基づいて、暗号化部により暗号化し、第 1 の暗号部分情報を生成し、前記平文を、前記一方向性関数に基づいて、第 1 の一方向性関数部により第 2 の暗号部分情報を生成し、前記第 1 の暗号部分情報と前記第 2 の暗号部分情報を連結して、暗号文として前記受信側に送信する暗号装置を備え、前記受信側では、受信した前記暗号文のうち前記第 1 の暗号部分情報を、前記復号鍵に基づいて、復号化部により復号し、第 1 の復号部分情報を生成し、前記第 1 の復号部分情報から、情報除去部により前記付加情報を除去し、第 2 の復号部分情報を生成し、前記第 2 の復号部分情報を、前記一方向性関数に基づいて、前記第 1 の一方向性関数部と同じ動作を行う第 2 の一方向性関数部により第 3 の復号部分情報を生成し、前記第 3 の復号部分情報が前記第 2 の暗号部分情報と等しい場合は、前記第 2 の復号部分情報を復号文とする復号装置を備えることを特徴とする。

## 【 0 0 2 6 】

請求項 5 における発明は、請求項 4 に記載の暗号装置は、平文に、情報付加部により付加情報を付加し、中間情報を生成し、前記中間情報を、請求項 4 に記載の暗号鍵に基づいて、暗号化部により暗号化し、第 1 の暗号部分情報を生成し、前記中間情報を、請求項 4 に記載の一方向性関数に基づいて、第 1 の一方向性関数部により第 2 の暗号部分情報を生成し、前記第 1 の暗号部分情報と前記第 2 の暗号部分情報を連結して、暗号文として送信することを特徴とする。

## 【 0 0 2 7 】

請求項 6 における発明は、請求項 4 に記載の復号装置は、受信した暗号文のうち第 1 の暗号部分情報を、請求項 4 に記載の復号鍵に基づいて、復号化部により復号し、第 1 の復号部分情報を生成し、前記第 1 の復号部分情報から、情報除去

部により前記付加情報を除去し、第2の復号部分情報を生成し、前記第2の復号部分情報を、請求項4に記載の一方方向性関数に基づいて、請求項4に記載の第1の一方方向性関数部と同じ動作を行う第2の一方方向性関数部により、第3の復号部分情報を生成し、前記第3の復号部分情報が受信した暗号文のうちの第2の暗号部分情報と等しい場合は、前記第2の復号部分情報を復号文とすることを特徴とする。

## 【0028】

請求項7における発明は、請求項1または請求項4に記載のデータ暗号化システムは、暗号化部で用いられる暗号方式が、公開鍵暗号方式であることを特徴とする。

## 【0029】

請求項8における発明は、請求項1または請求項4に記載のデータ暗号化システムは、第1の一方方向性関数部で用いられる一方方向性関数が、ハッシュ関数であることを特徴とする。

## 【0030】

請求項9における発明は、請求項1または請求項4に記載のデータ暗号化システムは、第1の一方方向性関数部で用いられる一方方向性関数が、秘密鍵暗号方式の暗号化関数であることを特徴とする。

## 【0031】

## 【発明の実施の形態】

## (実施の形態1)

図1は、実施の形態1における復号誤りが発生し得る暗号方式における復号誤り検出が可能であるデータ暗号化システム1000の構成を示すブロック図である。

## 【0032】

## (データ暗号化システム1000の構成)

データ暗号化システム1000は、復号誤りが発生し得る暗号方式における復号誤り検出が可能であるシステムであり、暗号装置1100、復号装置1200、及び通信路1300から構成される。ここでは、復号誤りが発生し得る暗号方



式として、NTRU暗号方式を用いた構成例を与える。NTRU暗号、及びNTRU暗号方式の暗号鍵、及び復号鍵の生成方法については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998.に詳しく述べられている。

## 【0033】

(暗号装置1100の構成)

図2は、暗号装置1100の構成を示すブロック図である。暗号装置1100は、暗号化部1110、第1の一方向性関数部1120、及び送信部1130を備える。ここでは、暗号化部1110としてNTRU暗号方式を用い、第1の一方向性関数部1120としてハッシュ関数を用いた構成例を与える。暗号装置1100は、平文 $m$ を入力とし、 $m$ に対する第1の暗号部分情報であるNTRU暗号方式による暗号文 $c (= E(m, K_p, r))$ と、第2の暗号部分情報であるハッシュ関数値 $h(m)$ を連結して出力する。

## 【0034】

(暗号化部1110)

図3は、暗号化部1110の構成を示すブロック図である。暗号化部1110は、NTRU暗号方式の暗号化を行うものであり、暗号化関数部1111、及び乱数生成部1112を備え、予め暗号化に用いる暗号鍵 $K_p$ が与えられているものとする。暗号化部1110は、入力として平文 $m$ が与えられたとき、乱数生成部1112で乱数 $r$ を生成し、予め与えられた暗号鍵 $K_p$ を用いて暗号化する際に、乱数 $r$ をパラメータとして使用して、平文 $m$ を暗号化関数部1111で暗号化した結果 $E(m, K_p, r)$ を生成し、送信部1130に入力する。以下、実施の形態1において、

$$c = E(m, K_p, r)$$

とする。ここで、上記乱数の例としては、C言語のライブラリ関数である $rand()$ が挙げられる。

## 【0035】

(第1の一方向性関数部1120)

第1の一方方向性関数部1120は、予め一方方向性関数としてハッシュ関数 $h$ が与えられているものとする。第1の一方方向性関数部1120は、上記平文 $m$ のハッシュ関数 $h$ の値 $h(m)$ を生成し、送信部1130に入力する。

## 【0036】

ここで、一方方向性関数とは、関数値を計算することは容易であるが、関数値から関数に入力された元の値を求めることが困難な関数のことである。また、ここで用いるハッシュ関数 $h$ は、関数の値 $h(m)$ から平文 $m$ の値を得ることが困難であるような十分に安全なもので、かつ衝突困難なものとする。一方方向性関数、ハッシュ関数、ハッシュ関数の安全性、及びハッシュ関数の衝突困難性については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、1997、56ページ及び189～195ページに詳しく述べられている。

## 【0037】

(送信部1130)

送信部1130は、暗号化部1110から入力された暗号文 $c$ と第1の一方方向性関数部1120から入力された $h(m)$ を連結して通信路1300に送信する。

## 【0038】

(復号装置1200の構成)

図4は、復号装置1200の構成を示すブロック図である。復号装置1200は、入力として暗号文 $c$ とハッシュ関数値 $h(m)$ を受け取り、復号文 $m'$ (= $D(c, K_s)$ )と復号誤り検出結果 $j$ を出力する。復号装置1200は、復号化部1210、第2の一方方向性関数部1220、受信部1230、及び比較部1240を備える。

## 【0039】

(復号化部1210)

図5は、復号化部1210の構成を示すブロック図である。復号化部1210は、暗号化部1110で用いられた暗号方式の復号を行うものであり、復号化関数部1211を備え、予め復号に用いる復号鍵 $K_s$ が与えられているものとする。復号化部1210は、入力として上記暗号文 $c$ が与えられたとき、予め与えら

れた復号鍵  $K_s$  を用いて、暗号文  $c$  を復号化関数部 1 2 1 1 で復号した結果  $D(c, K_s)$  を生成し、第 2 の一方向性関数部 1 2 2 0 に入力する。以下、実施の形態 1 において、

$$m' = D(c, K_s)$$

とする。

#### 【0 0 4 0】

(第 2 の一方向性関数部 1 2 2 0)

第 2 の一方向性関数部 1 2 2 0 は、第 1 の一方向性関数部 1 1 2 0 と同じ動作を行うものであり、予め一方向性関数としてハッシュ関数  $h$  が与えられているものとする。第 2 の一方向性関数部 1 2 2 0 は、上記復号結果  $m'$  のハッシュ関数  $h$  の値  $h(m')$  を生成し、比較部 1 2 4 0 に入力する。

#### 【0 0 4 1】

(受信部 1 2 3 0)

受信部 1 2 3 0 は、通信路 1 3 0 0 から連結された入力  $c$ 、 $h(m)$  を受け取り、 $c$  を復号化部 1 2 1 0 に、 $h(m)$  を比較部 1 2 4 0 にそれぞれ入力する。

#### 【0 0 4 2】

(比較部 1 2 4 0)

比較部 1 2 4 0 は、 $h(m)$  と  $h(m')$  を入力として、 $h(m)$  と  $h(m')$  が等しいかどうか比較し、等しい場合は  $j = 1$  とし、等しくない場合は  $j = 0$  をとして、比較結果  $j$  を出力する。

#### 【0 0 4 3】

(通信路 1 3 0 0 の構成)

通信路 1 3 0 0 は、暗号装置 1 1 0 0 と復号装置 1 2 0 0 との間のデータのやり取りが可能であるような通信路である。例えば、無線通信路やインターネットである。

#### 【0 0 4 4】

(データ暗号化システム 1 0 0 0 の動作)

データ暗号化システム 1 0 0 0 の全体の動作について、図 1、図 2、図 4 と、以下に述べる処理順序を用いて説明する。ここで、暗号鍵  $K_p$ 、復号鍵  $K_s$ 、及

び一方向性関数  $h$  は予め適切な方法で生成され、暗号鍵  $K_p$  は暗号化部 1 1 1 0 に格納され、復号鍵  $K_s$  は復号化部 1 2 1 0 に格納され、一方向性関数  $h$  は第 1 の一方向性関数部 1 1 2 0 及び第 2 の一方向性関数部 1 2 2 0 に与えられているものとする。

## 【0045】

暗号装置 1 1 0 0 は、入力として平文  $m$  を受け取る（ステップ S 1 0 1）。暗号化部 1 1 1 0 は、入力された  $m$  に対し、 $c = E(m, K_p, r)$  を生成し、送信部 1 1 3 0 に入力する（ステップ S 1 0 2）。第 1 の一方向性関数部 1 1 2 0 は、入力された  $m$  に対し、 $h(m)$  を生成し、送信部 1 1 3 0 に入力する（ステップ S 1 0 3）。送信部 1 1 3 0 は、入力された  $c$ 、及び  $h(m)$  を連結して暗号文とし、通信路 1 3 0 0 に送信する（ステップ S 1 0 4）。

## 【0046】

受信部 1 2 3 0 は、通信路 1 3 0 0 から暗号文である連結された  $c$ 、及び  $h(m)$  を受信し、 $c$  を復号化部 1 2 1 0 に、 $h(m)$  を比較部 1 2 4 0 にそれぞれ入力する（ステップ S 1 0 5）。復号化部 1 2 1 0 は、入力された  $c$  に対し、 $m' = D(c, K_s)$  を生成し、第 2 の一方向性関数部 1 2 2 0 に入力する（ステップ S 1 0 6）。第 2 の一方向性関数部 1 2 2 0 は、入力された  $m'$  に対し、 $h(m')$  を生成し、比較部 1 2 4 0 に入力する（ステップ S 1 0 7）。比較部 1 2 4 0 は、入力された  $h(m')$  と  $h(m)$  が等しいかどうかを判定し、等しい場合は  $j = 1$  とし、等しくない場合は  $j = 0$  として、比較結果  $j$  を出力する（ステップ S 1 0 8）。

## 【0047】

復号装置 1 2 0 0 は、復号化部 1 2 1 0 で出力された  $m'$  と比較部 1 2 4 0 で出力された  $j$  を復号文として出力する（ステップ S 1 0 9）。

## 【0048】

（実施の形態 1 における動作検証と従来例との比較）

以下に、この例の復号誤りの検出について説明する。以下で従来の方法との比較を行う。この例では、復号誤りが発生していない場合は、復号装置 1 2 0 0 内の比較部 1 2 4 0 の出力  $j$  は常に 1 である。

## 【0049】

また、復号誤りが発生している場合に、復号装置1200内の比較部1240の出力jが1となる確率、即ち、復号装置1200内の第2の一方向性関数部1220によって生成された $h(m')$ が、暗号装置1100内の第1の一方向性関数部1120によって生成された $h(m)$ と偶然等しくなる確率は、出力がkビットのハッシュ関数を第1の一方向性関数部1120、及び第2の一方向性関数部1220に用いた場合、kビットの出力は $2^k$ 通り存在するので、 $2^{-(k)}$ と等しい。ここで、 $a^b$ はaをb乗した結果を表す。

## 【0050】

従って、実際に復号誤りが発生したとき、復号装置1200から出力されるjを調べることによって、確率 $1 - 2^{-(k)}$ で復号誤りが発生したことを確認することができる。例えば、第1の一方向性関数部1120、及び第2の一方向性関数部1220で用いるハッシュ関数をSHA-1としたとき、SHA-1は160ビットの出力を持つので、この確率は $1 - 2^{-(160)}$ となり、ほぼ復号誤りの発生を検出することができる。SHA-1については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、1997、189～195ページに詳しく述べられている。

## 【0051】

また、通信量は、暗号化部1110の出力ビット長と第1の一方向性関数部1120の出力ビット長を合わせた量である。一般にハッシュ関数の出力ビット長は暗号文の出力ビット長よりも小さいので、この例での通信量は、暗号文の出力ビット長の2倍を越えない。例えば、ハッシュ関数にSHA-1を使った場合、現在、NTRU暗号方式を含む暗号方式は暗号文長が160ビット以上のものが使われることが多いので、このことは成り立つ。

## 【0052】

従来例2のデータ暗号化システムの通信量は、暗号文の出力ビット長の複数倍であったので、従来例2のデータ暗号化システムに比べて、この例では通信量が少なくなり、通信効率が向上する。さらに、安全性については、ハッシュ関数は、出力の値から入力得ることは困難であり、また、従来例2のように同じ

平文を複数回送信することはないので、十分な安全性が確保できる。

【0053】

(実施の形態1の変形例)

以上、データ暗号化システムにおいて、暗号化部にNTRU暗号方式を適用し、第1の一方向性関数部にハッシュ関数を用いる実施の形態に基づいて説明したが、本発明は、この実施の形態に限られず、暗号化部に、DES暗号方式、RSA暗号方式やElGamal暗号方式などの一般の暗号方式を適用でき、また第1の一方向性関数部には、ハッシュ関数以外に、前記一般の暗号方式の暗号化関数などの一方向性関数を用いてもよい。DES暗号方式、RSA暗号方式、及びElGamal暗号方式については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、1997に詳しく述べられている。さらに、システム利用者全体で一方向性関数を共有せずに、送信側及び受信側のユーザ組毎に一方向性関数が異なってもよい。

【0054】

また、本発明は、上記のデータ暗号化システムを実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラムまたは、前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、半導体メモリ、ICカードなどに記録したものとしてもよい。

【0055】

また、これらの記録媒体に記録されている前記コンピュータプログラムまたは、前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワークなどを經由して伝送するものとしてもよい。

【0056】

(実施の形態2)

図6は、実施の形態2における復号誤りが発生し得る暗号方式における復号誤

り検出が可能であるデータ暗号化システム2000の構成を示すブロック図である。

#### 【0057】

(データ暗号化システム2000の構成)

データ暗号化システム2000は、復号誤りが発生し得る暗号方式における復号誤り検出が可能であるシステムであり、暗号装置2100、復号装置2200、及び通信路2300から構成される。ここでは、復号誤りが発生し得る暗号方式として、NTRU暗号方式を用いた構成例を与える。

#### 【0058】

(暗号装置2100の構成)

図7は、暗号装置2100の構成を示すブロック図である。暗号装置2100は、暗号化部2110、第1の一方方向性関数部2120、送信部2130及び情報付加部2140を備える。ここでは、暗号化部2110としてNTRU暗号方式を用い、第1の一方方向性関数部2120としてハッシュ関数を用い、情報付加部2140として予め決められたビット数の乱数を付加する情報付加部を用いた構成例を与える。

#### 【0059】

暗号装置2100は、平文 $m$ を入力とし、 $m$ に対する第1の暗号部分情報である、NTRU暗号方式による暗号文 $c (= E(m || R_a, K_p, r))$ と第2の暗号部分情報であるハッシュ関数値 $h(m)$ を連結して出力する。

#### 【0060】

(暗号化部2110)

図8は、暗号化部2110の構成を示すブロック図である。暗号化部2110は、NTRU暗号方式の暗号化を行うものであり、暗号化関数部2111及び乱数生成部2112を備え、予め暗号化に用いる暗号鍵 $K_p$ が与えられているものとする。暗号化部2110は、情報付加部2140から入力として平文 $m || R_a$ が与えられたとき、乱数生成部2112で乱数 $r$ を生成し、予め与えられた暗号鍵 $K_p$ を用いて暗号化する際に、乱数 $r$ をパラメータとして使用して、平文 $m || R_a$ を暗号化関数部2111で暗号化した結果 $E(m || R_a, K_p, r)$

を生成し、送信部 2 1 3 0 に出力する。

#### 【0 0 6 1】

以下、実施の形態 2 において、

$$c = E(m \parallel Ra, Kp, r)$$

とする。ここで、上記乱数の例としては、C 言語のライブラリ関数である `rand()` が挙げられる。

#### 【0 0 6 2】

（第 1 の一方向性関数部 2 1 2 0）

第 1 の一方向性関数部 2 1 2 0 は、予め一方向性関数としてハッシュ関数  $h$  が与えられているものとする。第 1 の一方向性関数部 2 1 2 0 は、上記平文  $m$  のハッシュ関数  $h$  の値  $h(m)$  を生成し、送信部 2 1 3 0 に出力する。ここで用いるハッシュ関数  $h$  は、関数の値  $h(m)$  から平文  $m$  の値を得ることが困難であるような十分に安全なもので、かつ衝突困難なものとする。

#### 【0 0 6 3】

（送信部 2 1 3 0）

送信部 2 1 3 0 は、暗号化部 2 1 1 0 から出力された暗号文  $c$  と第 1 の一方向性関数部 2 1 2 0 から出力された  $h(m)$  を連結して通信路 2 3 0 0 に送信する。

#### 【0 0 6 4】

（情報付加部 2 1 4 0）

情報付加部 2 1 4 0 は、入力  $m$  が与えられたとき、予め決められたビット数  $rLen$  の長さの乱数  $Ra$  を生成して、 $m$  に  $Ra$  をビット結合した結果  $m \parallel Ra$  を算出し、暗号化部 2 1 1 0 に入力する。ここで、ビット結合という操作は、2 つの値をビット列で表現し、それらを結合したものを 1 つの値とする操作である。例えば、 $m = 10$ 、 $rLen = 5$ 、 $Ra = 7$  とすると、 $m$  のビット列表現は  $1010$ 、 $Ra$  の長さ  $rLen$  のビット列表現は  $00111$  となるので、ビット結合した結果は、 $101000111$  となり、これは十進数で  $327$  である。

#### 【0 0 6 5】

（復号装置 2 2 0 0 の構成）



図9は、復号装置2200の構成を示すブロック図である。復号装置2200は、入力として暗号文 $c$ とハッシュ関数値 $h(m)$ を受け取り、復号文 $m'$ と復号誤り検出結果 $j$ を出力する。復号装置2200は、復号化部2210、第2の一方方向性関数部2220、受信部2230、比較部2240、及び情報除去部2250を備える。

## 【0066】

(復号化部2210)

図10は、復号化部2210の構成を示すブロック図である。復号化部2210は、暗号化部2110で用いられた暗号方式の復号を行うものであり、復号化関数部2211を備え、予め復号に用いる復号鍵 $K_s$ が与えられているものとする。復号化部2210は、入力として上記暗号文 $c$ が与えられたとき、予め与えられた復号鍵 $K_s$ を用いて、暗号文 $c$ を復号化関数部2211で復号した結果 $D(c, K_s)$ を生成し、情報除去部2250へ入力する。以下、実施の形態2において、

$$Ma = D(c, K_s)$$

とする。

## 【0067】

(第2の一方方向性関数部2220)

第2の一方方向性関数部2220は、第1の一方方向性関数部2120と同じ動作を行うものであり、予め一方方向性関数としてハッシュ関数 $h$ が与えられているものとする。第2の一方方向性関数部2220は、情報除去部2250によって入力された $m'$ のハッシュ関数 $h$ の値 $h(m')$ を生成し、比較部2240に出力する。

## 【0068】

(受信部2230)

受信部2230は、通信路2300から連結された入力 $c, h(m)$ を受け取り、 $c$ を復号化部2210に、 $h(m)$ を比較部2240にそれぞれ入力する。

## 【0069】

(比較部2240)

比較部 2 2 4 0 は、 $h(m)$  と  $h(m')$  を入力として、 $h(m)$  と  $h(m')$  が等しいかどうか比較し、等しい場合は  $j = 1$  とし、等しくない場合は  $j = 0$  として、比較結果  $j$  を出力する。

## 【0 0 7 0】

## (情報除去部 2 2 5 0)

情報除去部 2 2 5 0 は、復号化部 2 2 1 0 より入力  $Ma$  が与えられたとき、 $Ma$  をビット列表現した結果から情報付加部 2 1 4 0 で用いられたビット数  $rLen$  のビットを除去した結果を算出し、第 2 の一方向性関数部 2 2 2 0 に入力する。例えば、 $Ma = 327$ 、 $rLen = 5$  とすると、 $Ma$  のビット列表現は 1 0 1 0 0 0 1 1 1 となり、これから長さ  $rLen$  のビット 0 0 1 1 1 を除去すると、結果は 1 0 1 0 となり、これは十進数で 1 0 である。

## 【0 0 7 1】

## (通信路 2 3 0 0 の構成)

通信路 2 3 0 0 は、暗号装置 2 1 0 0 と復号装置 2 2 0 0 との間のデータのやり取りが可能であるような通信路である。例えば、無線通信路やインターネットである。

## 【0 0 7 2】

## (データ暗号化システム 2 0 0 0 の動作)

データ暗号化システム 2 0 0 0 の全体の動作について、図 6、図 7、図 9 と、以下に述べる処理順序を用いて説明する。ここで、暗号鍵  $K_p$ 、復号鍵  $K_s$ 、及び一方向性関数  $h$  は予め適切な方法で生成され、暗号鍵  $K_p$  は暗号化部 2 1 1 0 に格納され、復号鍵  $K_s$  は復号化部 2 2 1 0 に格納され、一方向性関数  $h$  は第 1 の一方向性関数部 2 1 2 0 及び第 2 の一方向性関数部 2 2 2 0 に与えられているものとする。

## 【0 0 7 3】

暗号装置 2 1 0 0 は、入力として平文  $m$  を受け取る (ステップ S 2 0 1)。情報付加部 2 1 4 0 は、入力された  $m$  に対し  $m || Ra$  を生成し、暗号化部 2 1 1 0 に入力する (ステップ S 2 0 2)。暗号化部 2 1 1 0 は、入力された  $m || Ra$  に対し、 $c = E(m || Ra, K_p, r)$  を生成し、送信部 2 1 3 0 に入力す

る（ステップ S 2 0 3）。第 1 の一方向性関数部 2 1 2 0 は、入力された  $m$  に対し、 $h(m)$  を生成し、送信部 2 1 3 0 に入力する（ステップ S 2 0 4）。送信部 2 1 3 0 は、入力された  $c$ 、及び  $h(m)$  を連結して暗号文とし、通信路 2 3 0 0 に送信する（ステップ S 2 0 5）。

## 【 0 0 7 4 】

受信部 2 2 3 0 は、通信路 2 3 0 0 から暗号文である連結された  $c$ 、及び  $h(m)$  を受信し、 $c$  を復号化部 2 2 1 0 に、 $h(m)$  を比較部 2 2 4 0 にそれぞれ入力する（ステップ S 2 0 6）。復号化部 2 2 1 0 は、入力された  $c$  に対し、 $M_a = D(c, K_s)$  を生成し、情報除去部 2 2 5 0 に入力する（ステップ S 2 0 7）。情報除去部 2 2 5 0 は、入力された  $M_a$  に対し、 $m'$  を生成し、第 2 の一方向性関数部 2 2 2 0 に入力する（ステップ S 2 0 8）。第 2 の一方向性関数部 2 2 2 0 は、入力された  $m'$  に対し、 $h(m')$  を生成し、比較部 2 2 4 0 に入力する（ステップ S 2 0 9）。比較部 2 2 4 0 は、入力された  $h(m')$  と  $h(m)$  が等しいかどうか判定し、等しい場合  $j = 1$ 、等しくない場合  $j = 0$  として、比較結果  $j$  を出力する（ステップ S 2 1 0）。

## 【 0 0 7 5 】

復号装置 2 2 0 0 は、情報除去部 2 2 5 0 で出力された  $m'$  と比較部 2 2 4 0 で出力された  $j$  を復号文として出力する（ステップ S 2 1 1）。

## 【 0 0 7 6 】

（実施の形態 2 における動作検証と従来例との比較）

以下に、この例の復号誤りの検出について説明する。以下で従来の方法との比較を行う。この例では、復号誤りが発生していない場合は、復号装置 2 2 0 0 内の比較部 2 2 4 0 の出力  $j$  は常に 1 である。

## 【 0 0 7 7 】

また、復号誤りが発生している場合に、復号装置 2 2 0 0 内の比較部 2 2 4 0 の出力  $j$  が 1 となる確率、即ち、復号装置 2 2 0 0 内の第 2 の一方向性関数部 2 2 2 0 によって生成された  $h(m')$  が、暗号装置 2 1 0 0 内の第 1 の一方向性関数部 2 1 2 0 によって生成された  $h(m)$  と偶然等しくなる確率は、出力が  $k$  ビットのハッシュ関数を第 1 の一方向性関数部 2 1 2 0、及び第 2 の一方向性関

数部 2220 に用いた場合、 $k$  ビットの出力は  $2^k$  通り存在するので、 $2^{(-k)}$  と等しい。

## 【0078】

従って、実際に復号誤りが発生したとき、復号装置 2200 から出力される  $j$  を調べることによって、確率  $1 - 2^{(-k)}$  で復号誤りが発生したことを確認することができる。例えば、第 1 の一方向性関数部 2120、及び第 2 の一方向性関数部 2220 で用いるハッシュ関数を SHA-1 としたとき、SHA-1 は 160 ビットの出力を持つので、この確率は  $1 - 2^{(-160)}$  となり、ほぼ復号誤りの発生を検出することができる。

## 【0079】

また、通信量は、暗号化部 2110 の出力ビット長と第 1 の一方向性関数部 2120 の出力ビット長を合わせた量である。一般にハッシュ関数の出力ビット長は暗号文の出力ビット長よりも小さいので、この例での通信量は、暗号文の出力ビット長の 2 倍を越えない。例えば、ハッシュ関数に SHA-1 を使った場合、現在、NTRU 暗号方式を含む暗号方式は暗号文長が 160 ビット以上のものが使われることが多いので、このことは成り立つ。

## 【0080】

従来例 2 のデータ暗号化システムの通信量は、暗号文の出力ビット長の複数倍であったので、従来例 2 のデータ暗号化システムに比べて、この例では通信量が少なくなり、通信効率が向上する。

## 【0081】

ここで、平文  $m$  は、長さ  $rLen$  の乱数  $Ra$  が付加されて、暗号化部 2110 に入力されるので、暗号装置 2100 に入力できる平文の長さは、実施の形態 1 のデータ暗号化システムよりも長さ  $rLen$  だけ短くなる。但し、暗号化部 2110 に暗号文長が 160 ビットの暗号方式を用いるとき、 $rLen$  を 32 ビットとしても、128 ビットのデータを送信できるため、実用上は問題ない。

## 【0082】

さらに、安全性については、ハッシュ関数は、出力の値から入力の値を得ることは困難であり、また、従来例 2 のように同じ平文を複数回送信することはない

ので、十分な安全性が確保できる。加えて、復号誤り検出の後に、再送要求を行い、同じデータを再度送信させるプロトコルを考えたときでも、平文に乱数が付加されて暗号化されているので、従来例2のMultiple Transmission Attackに対して、この例では従来例2のデータ暗号化システムよりも耐性を持っている。

## 【0083】

(実施の形態2の変形例)

以上、データ暗号化システムにおいて、暗号化部にNTRU暗号方式を適用し、第1の一方向性関数部にハッシュ関数を用い、情報付加部で乱数を付加する処理を行う実施の形態に基づいて説明したが、本発明は、この実施の形態に限られず、暗号化部に、DES暗号方式、RSA暗号方式やElGamal暗号方式などの一般の暗号方式を適用でき、また第1の一方向性関数部には、ハッシュ関数以外に、前記一般の暗号方式の暗号化関数などの一方向性関数を用いてもよい。加えて、情報付加部では、時間情報や定型情報など、任意の情報を付加する処理を行ってもよい。DES暗号方式、RSA暗号方式、及びElGamal暗号方式については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、1997に詳しく述べられている。さらに、システム利用者全体で一方向性関数を共有せずに、送信側及び受信側のユーザ組毎に一方向性関数が異なってもよい。

## 【0084】

また、本発明は、上記の公開鍵暗号方法を実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラムまたは、前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、半導体メモリ、ICカードなどに記録したものとしてもよい。

## 【0085】

また、これらの記録媒体に記録されている前記コンピュータプログラムまたは、前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラムまたは前記デジタル信号を、電気通信回線、無線または有線通信回線、

インターネットを代表とするネットワークなどを経由して伝送するものとしてもよい。

【 0 0 8 6 】

【発明の効果】

以上に説明したように本発明は、従来例における問題点を鑑みて行われたもので、復号誤りの発生し得る暗号方式において、安全で、効率的に、かつほぼ完全に復号誤りの検出が可能となった。以上により、実用的な復号誤りの検出装置を提供することができ、その価値は大きい。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 のデータ暗号化システムのブロック図

【図 2】

本発明の実施の形態 1 の暗号装置のブロック図

【図 3】

本発明の実施の形態 1 の暗号化部のブロック図

【図 4】

本発明の実施の形態 1 の復号装置のブロック図

【図 5】

本発明の実施の形態 1 の復号化部のブロック図

【図 6】

本発明の実施の形態 2 のデータ暗号化システムのブロック図

【図 7】

本発明の実施の形態 2 の暗号装置のブロック図

【図 8】

本発明の実施の形態 2 の暗号化部のブロック図

【図 9】

本発明の実施の形態 2 の復号装置のブロック図

【図 1 0】

本発明の実施の形態 2 の復号化部のブロック図

【図 1 1】

従来例 1 のデータ暗号化システムのブロック図

【図 1 2】

従来例 1 の暗号装置のブロック図

【図 1 3】

従来例 1 の暗号化部のブロック図

【図 1 4】

従来例 1 の復号装置のブロック図

【図 1 5】

従来例 1 の復号化部のブロック図

【図 1 6】

従来例 2 のデータ暗号化システムのブロック図

【図 1 7】

従来例 2 の暗号装置のブロック図

【図 1 8】

従来例 2 の暗号化部のブロック図

【図 1 9】

従来例 2 の復号装置のブロック図

【図 2 0】

従来例 2 の復号化部のブロック図

【符号の説明】

1 0 0 0, 2 0 0 0, 3 0 0 0, 4 0 0 0 データ暗号化システム  
 1 1 0 0, 2 1 0 0, 3 1 0 0, 4 1 0 0 暗号装置  
 1 1 1 0, 2 1 1 0, 3 1 1 0, 4 1 1 0 暗号化部  
 1 1 1 1, 2 1 1 1, 3 1 1 1, 4 1 1 1 暗号化関数部  
 1 1 1 2, 2 1 1 2, 3 1 1 2, 4 1 1 2 乱数生成部  
 1 1 2 0, 2 1 2 0 第 1 の一方向性関数部  
 1 1 3 0, 2 1 3 0, 3 1 2 0, 4 1 2 0 送信部  
 1 2 0 0, 2 2 0 0, 3 2 0 0, 4 2 0 0 復号装置

1210, 2210, 3210, 4210 復号化部

1211, 2211, 3211, 4211 復号化関数部

1220, 2220 第2の一方方向性関数部

1230, 2230, 3220, 4220 受信部

1240, 2240, 4230 比較部

1300, 2300, 3300, 4300 通信路

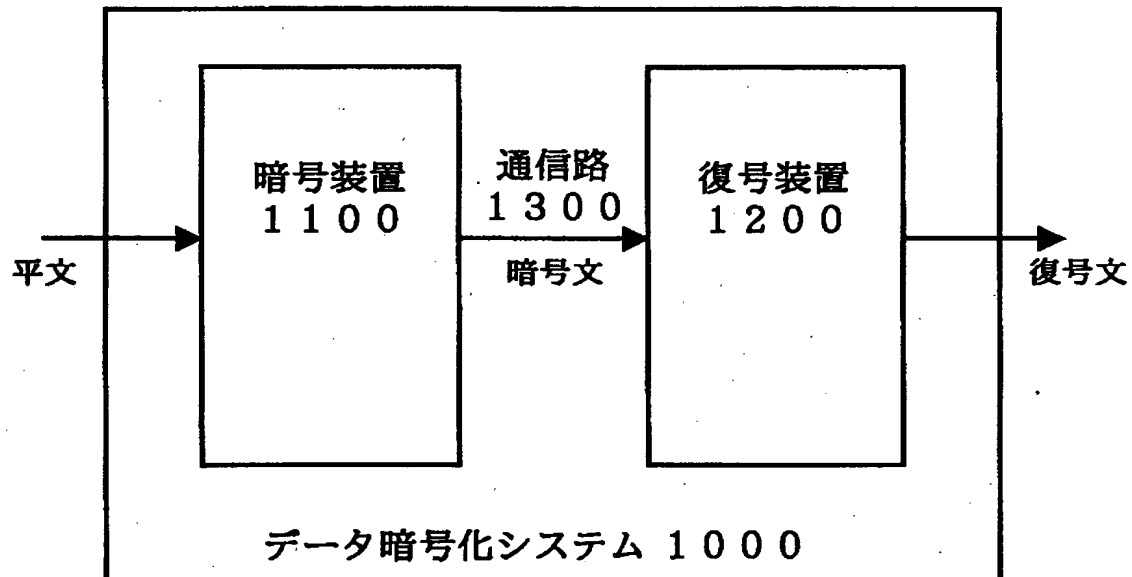
2140 情報付加部

2250 情報除去部

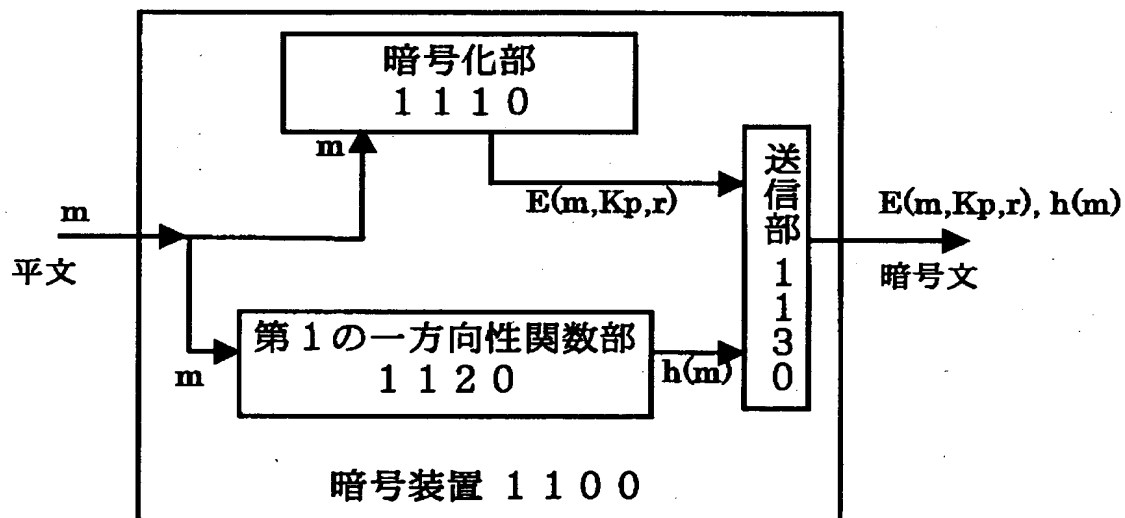


【書類名】 図面

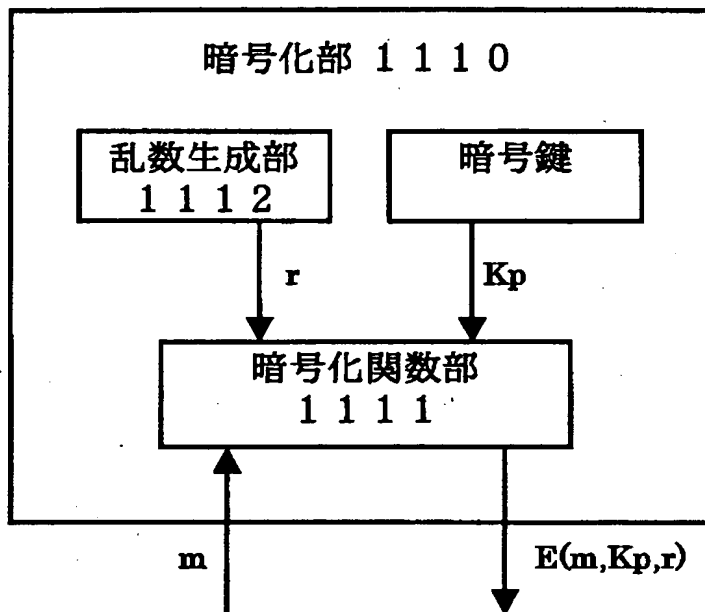
【図 1】



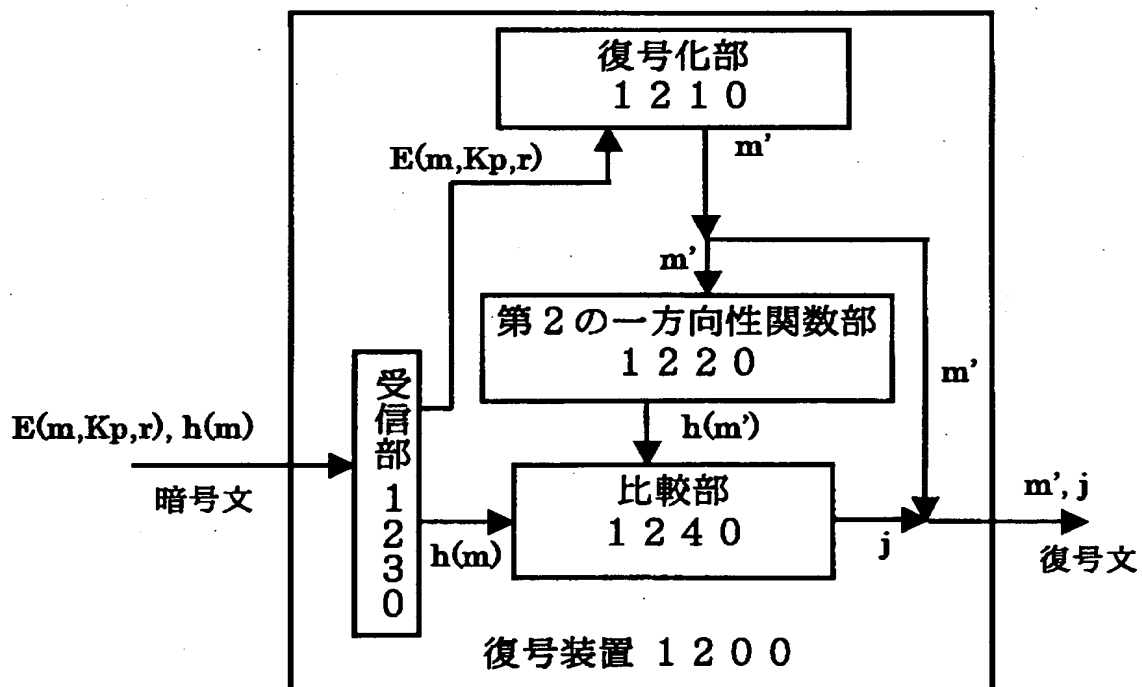
【図 2】



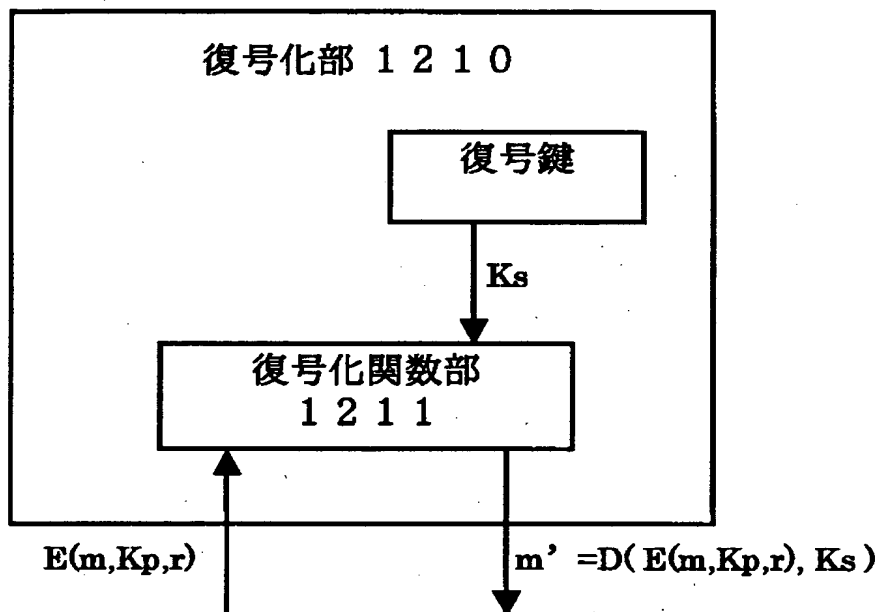
【図 3】



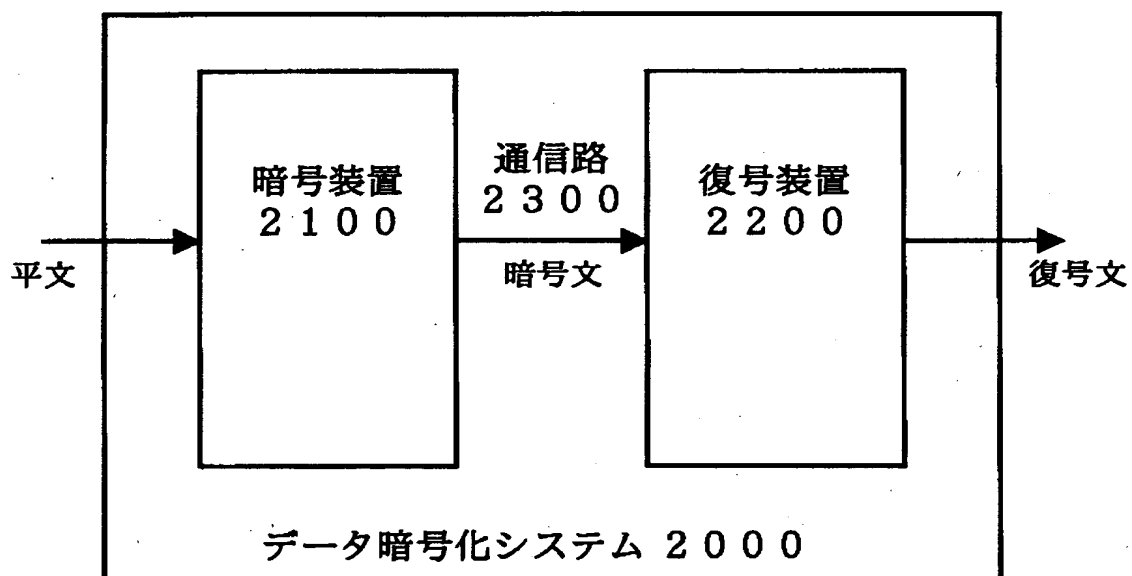
【図 4】



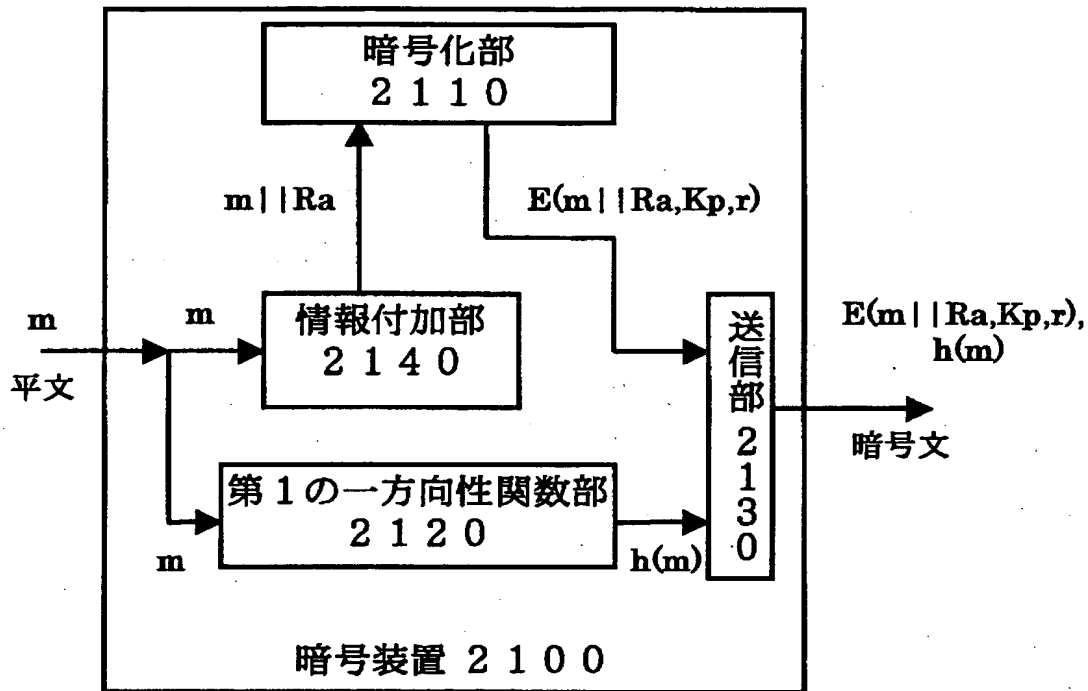
【図 5】



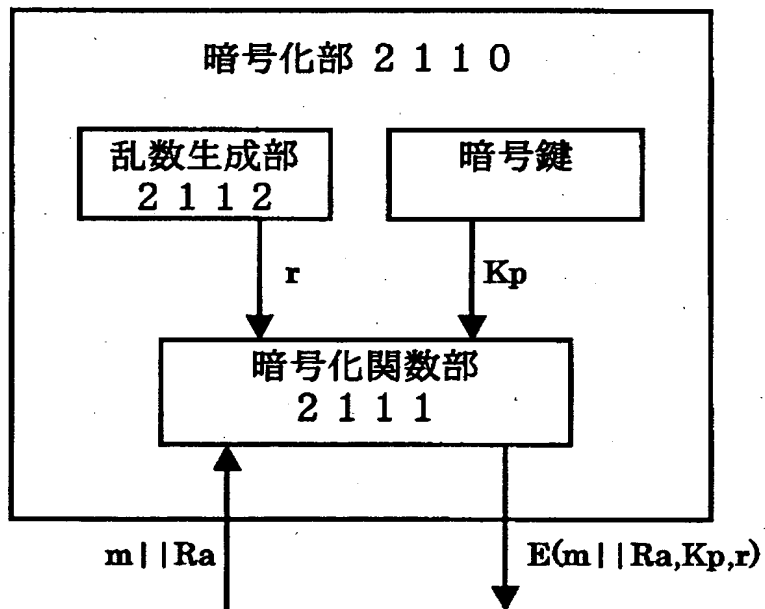
【図 6】



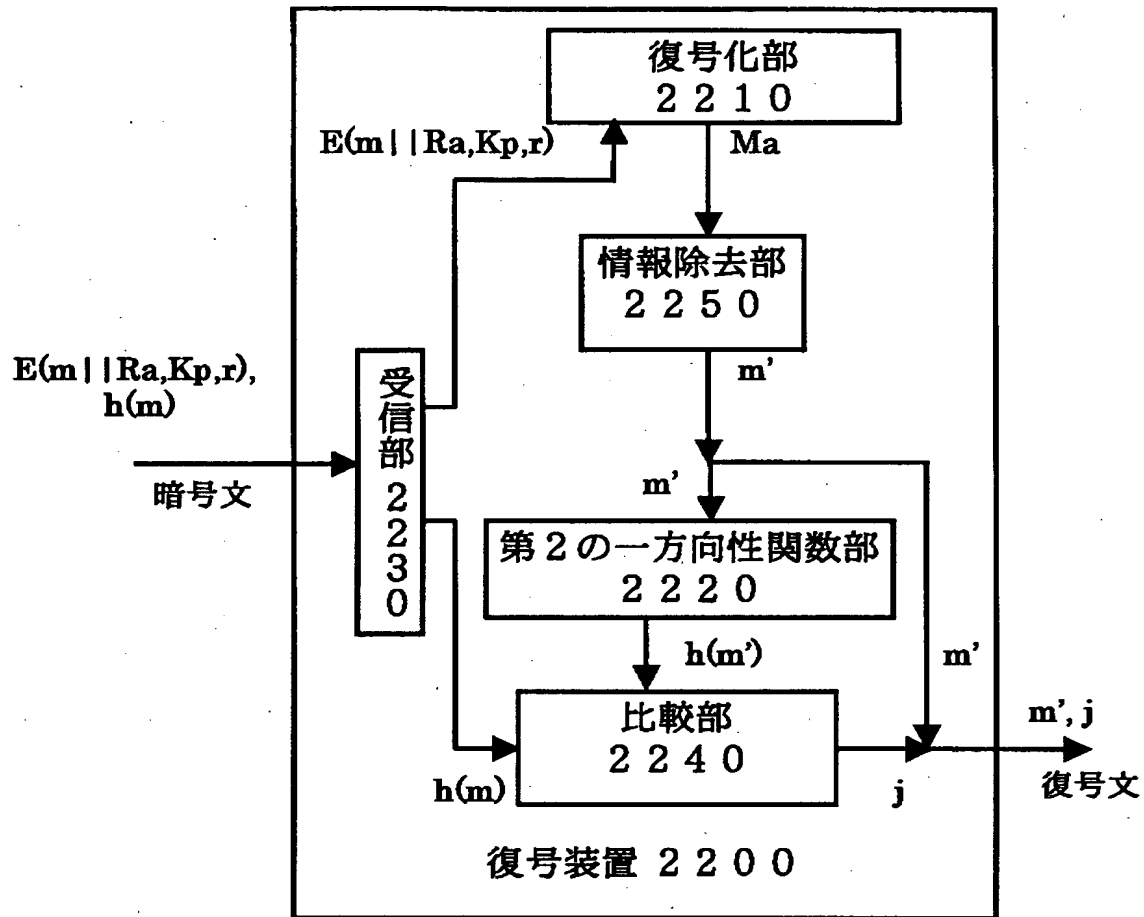
【図 7】



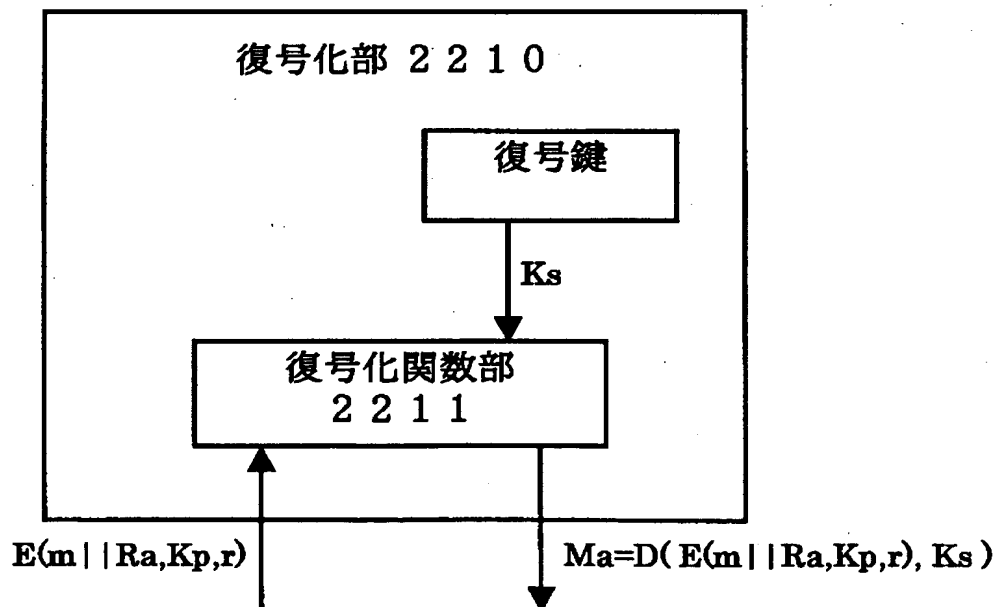
【図 8】



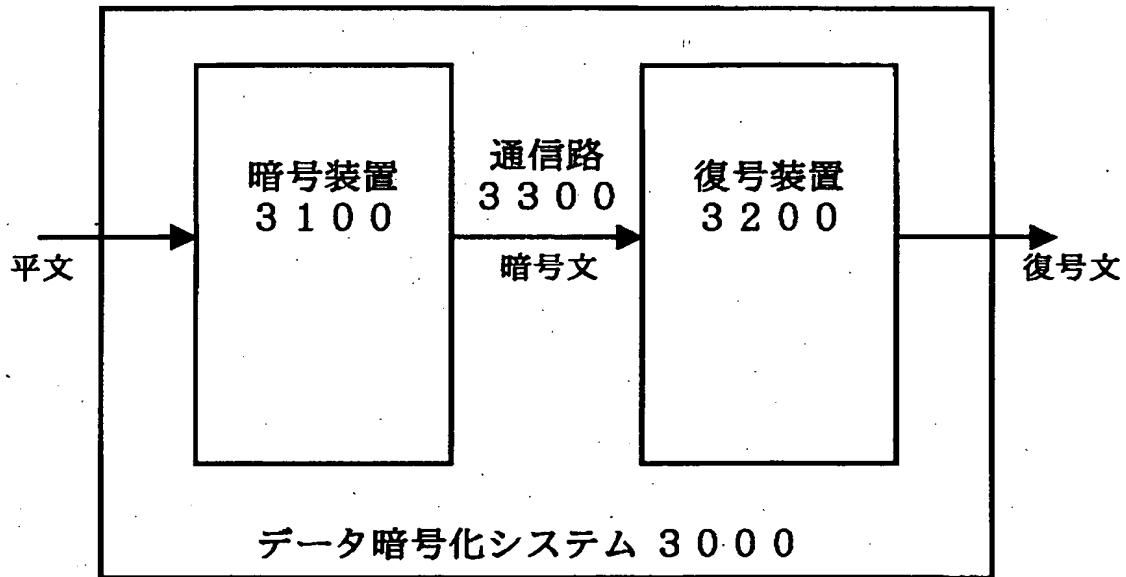
【図 9】



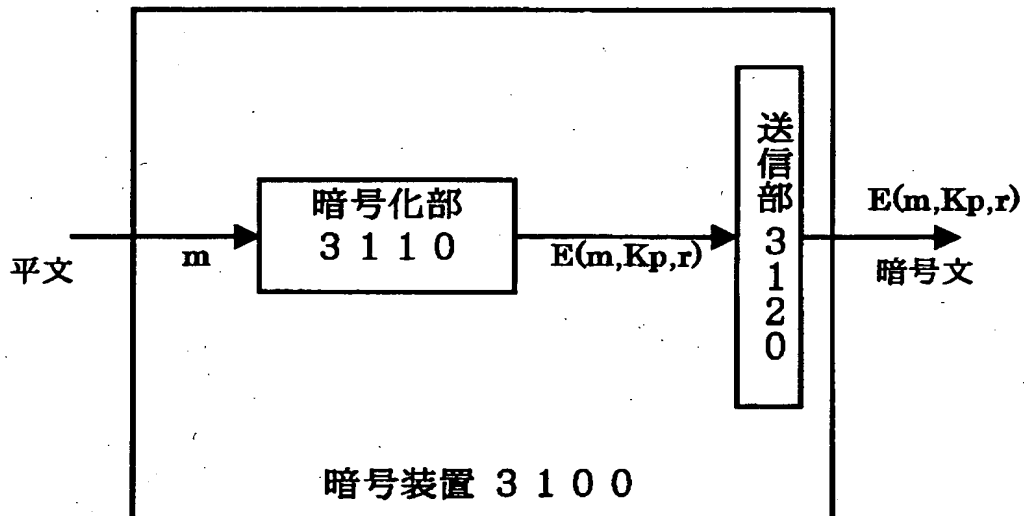
【図 10】



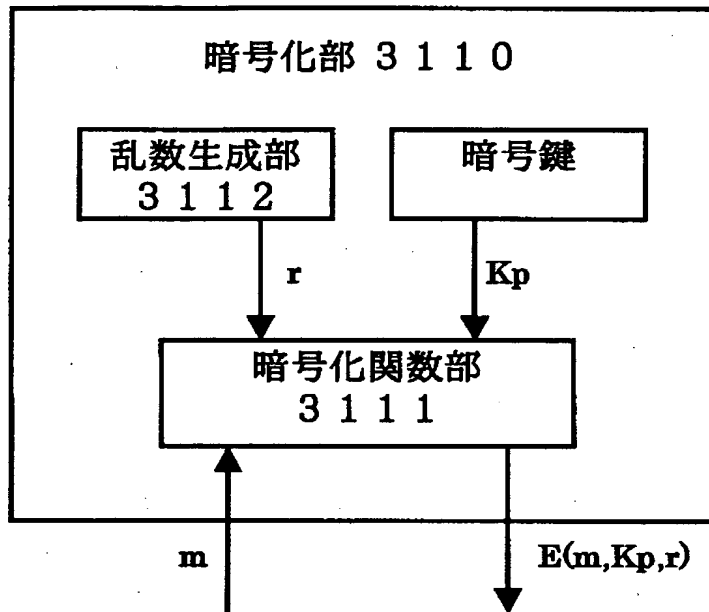
【図 1 1】



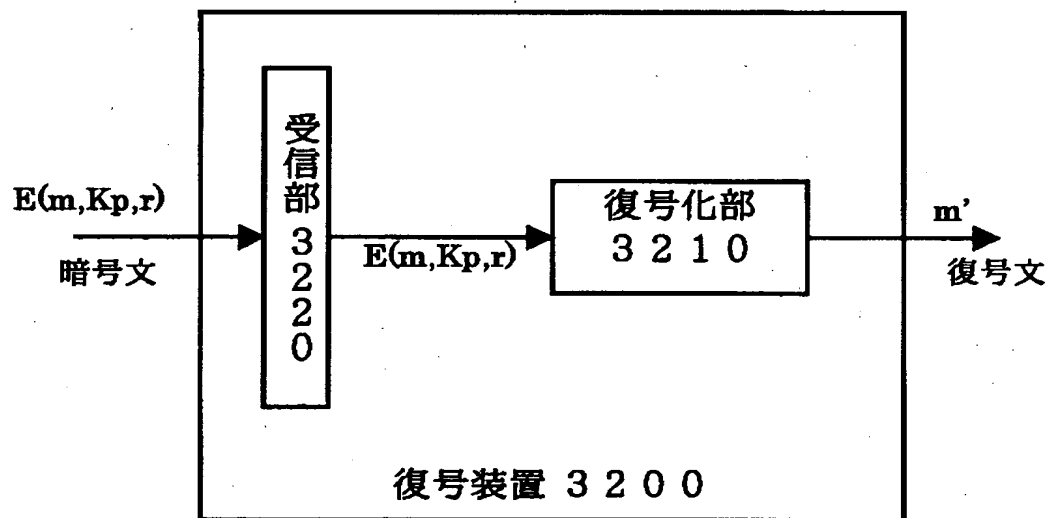
【図 1 2】



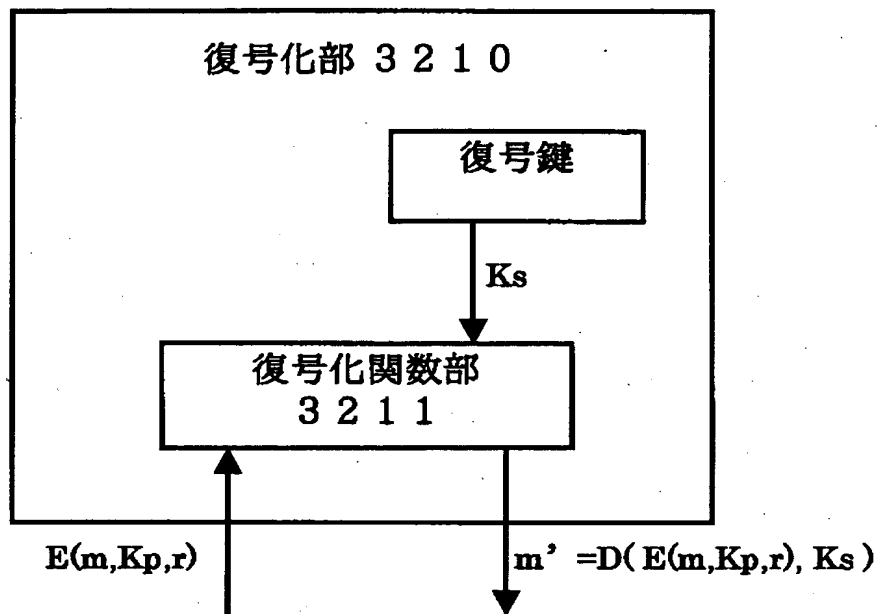
【図 1 3】



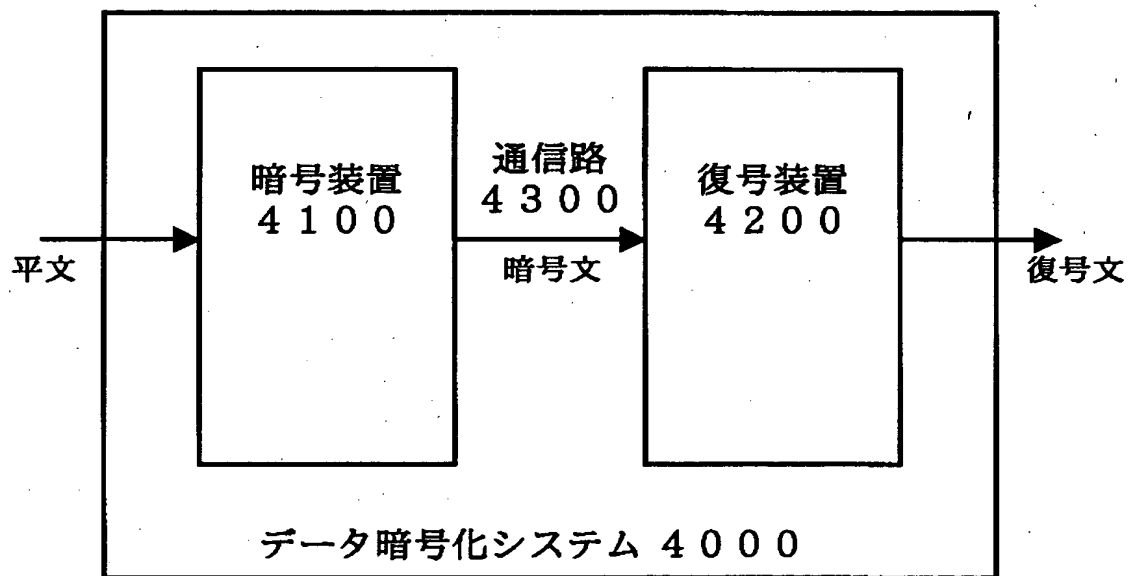
【図 1 4】



【図 1 5】

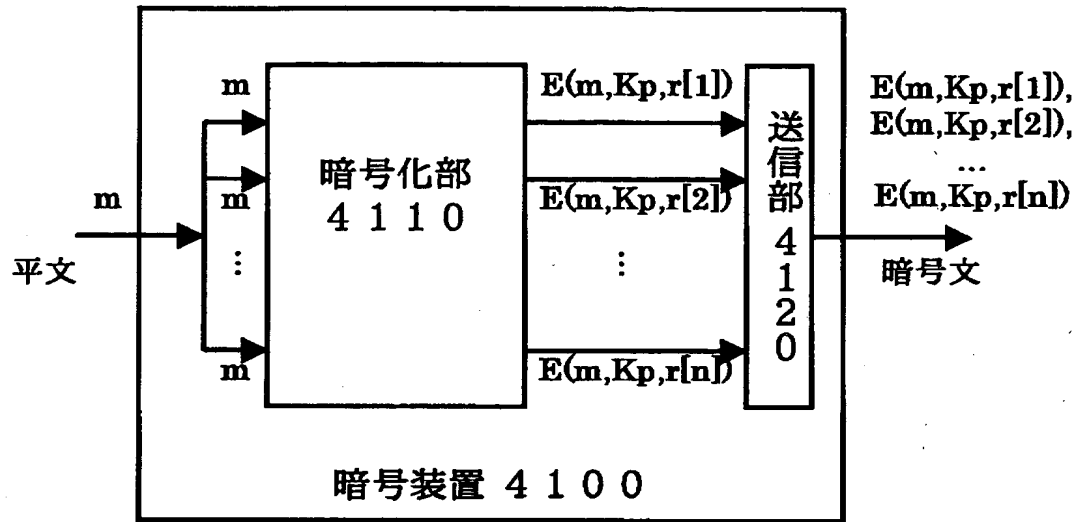


【図 1 6】

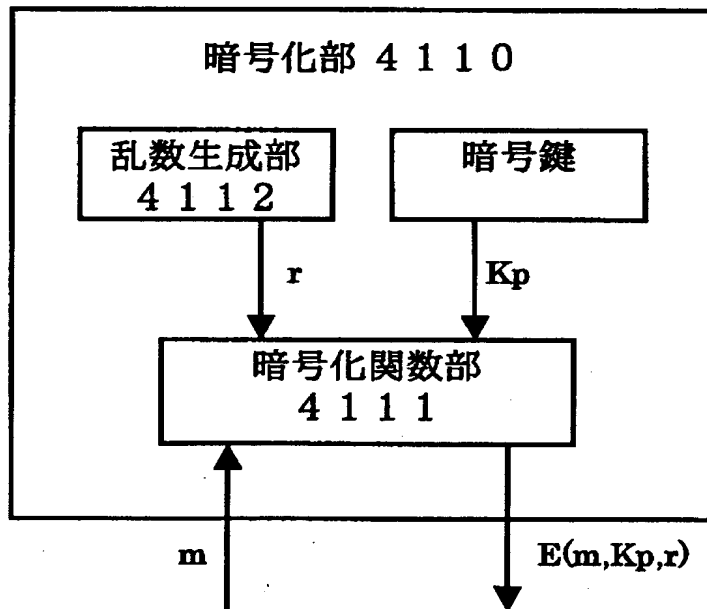




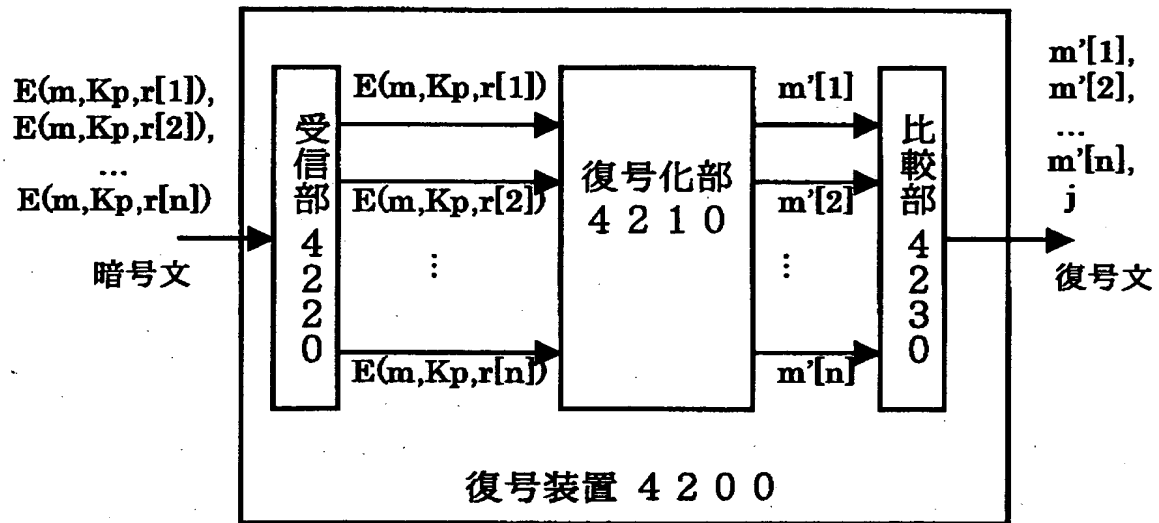
【図 1 7】



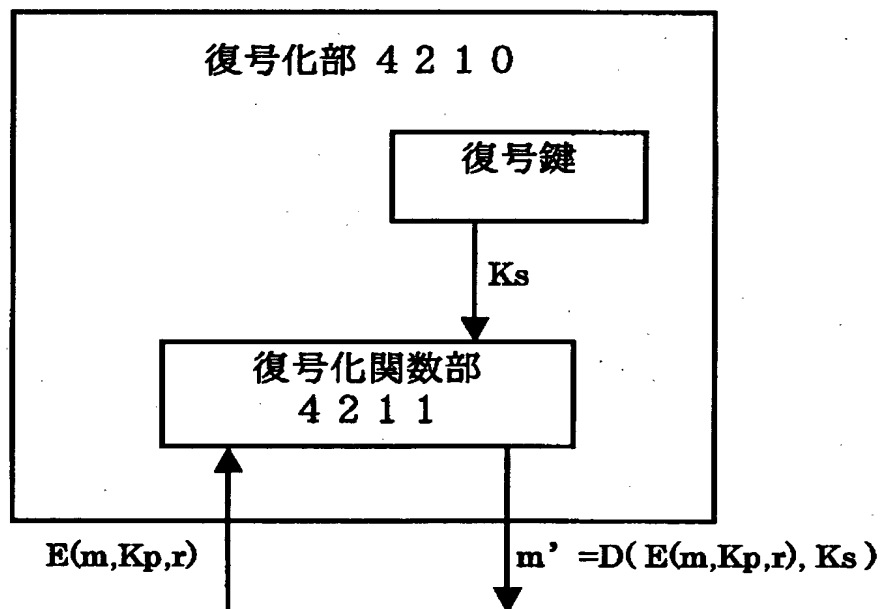
【図 1 8】



【図 1 9】



【図 2 0】



【書類名】 要約書

【要約】

【課題】 データ暗号化システムにより、安全で効率的に復号誤りを検出する技術を提供することを目的とする。

【解決手段】 本発明は、送信側と受信側で予め対となる暗号鍵と復号鍵、また一方向性関数を定めておき、送信側で平文を、暗号鍵と一方向性関数に基づき暗号化して暗号文を生成し、暗号文を受信側に送信し、受信側では復号鍵と一方向性関数に基づいて暗号文を復号し、復号文を入手することを特徴とする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社